World of Tech WOT | 51CTO传媒

WOT 2015 互联网运维与开发者大会

■ 2015年04月10日-11日 ■ 北京珠三角JW万豪酒店

构建安全监控平台

关于我:

lion_00
CCIE　2011年11月
CISSP　2013年4月
安全爱好者

安全监控应该怎么做

开源/商业

大量的告警有人看吗

怎么才可以让告警准确一些

监控的范围以及层次

以核心资源为中心进行保护

尽量将所有边界囊括其中

一 网络层

数据源:出口流量镜像

IDS:suricata　　简单展示界面:BASE　　报表展示：SNORBY

网络IDS 起到了眼睛的作用，绝大多数攻击
可以通过编辑网络IDS的规则便可以发现，比如SQLMAP，AWVS等等。

二 日志的存储与展示

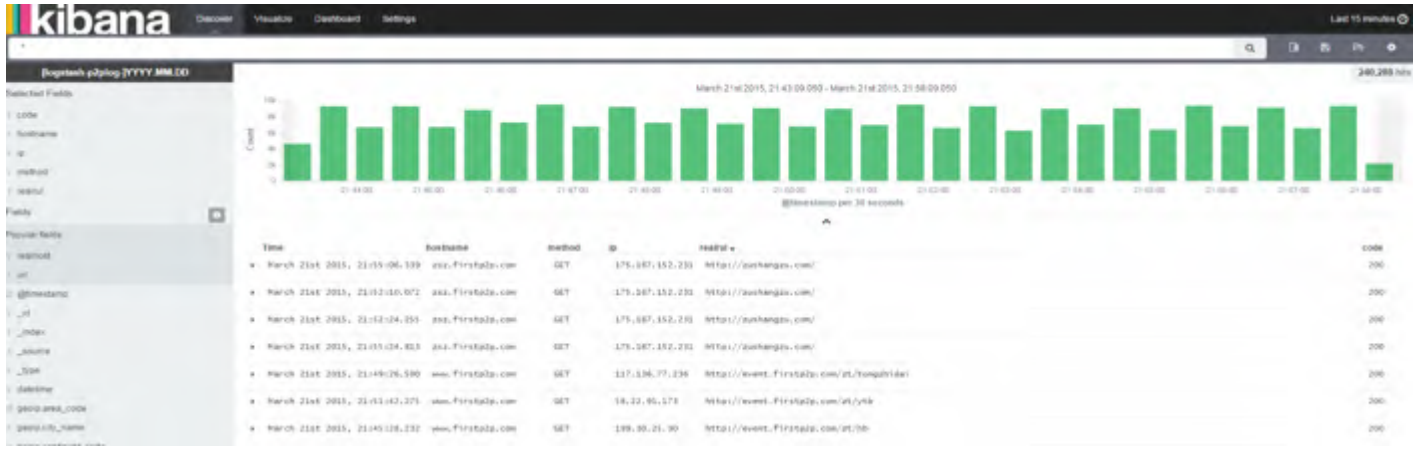
数据源:出口流量镜像

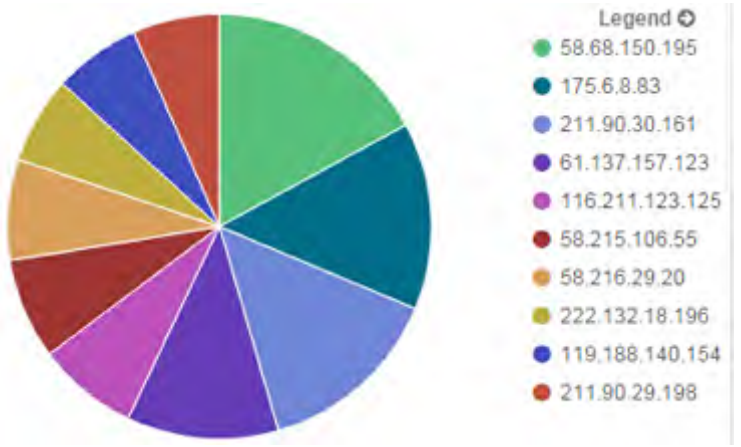
将外部访问的HTTP/HTTPS数据从网络流量中提取出来，以便后续使用

{ "src": "1.93.50.136:1117", "dst": "[redacted]", "method": "GET", "url": "\/statics\/js\/formvalidatorregex.js", "referer": "http:\/
\/[redacted]\/index.php?m=yuegao&c=index&a=yuegao_show", "user-agent": "Mozilla\/4.0 (compatible; MSIE 9.0; Windows NT 6.1; SV1; .NET CL
R 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; 360SE)", "host": "[redacted]", "cookie": "PHPSESSID=qja0t7k5
pun[redacted]7", "code": 200, "time": 1410771195 }
{ "src": "1.93.50.136:1118", "dst": "[redacted]", "method": "GET", "url": "\/statics\/js\/jquery.validate.js", "referer": "http:\/\/n
[redacted]c\/index.php?m=yuegao&c=index&a=yuegao_show", "user-agent": "Mozilla\/4.0 (compatible; MSIE 9.0; Windows NT 6.1; SV1; .NET CLR 1
.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; 360SE)", "host": "[redacted]", "cookie": "PHPSESSID=qja0t7k5pun
6[redacted]7", "code": 200, "time": 1410771195 }
{ "src": "182.202.248.183:4014", "dst": "[redacted]", "method": "GET", "url": "\/count.js?siteid=701", "referer": "http:[redacted].
cn\/?track=588|2564", "user-agent": "Mozilla\/4.0 (compatible; MSIE 6.1; Windows XP; .NET CLR 1.1.4322; .NET CLR 2.0.50727)", "host": "sta
t[redacted]", "code": 200, "time": 1410771195 }
{ "src": "113.200.250.39:1891", "dst": "[redacted]", "method": "GET", "url": "\/?track=588|2743", "user-agent": "Mozilla\/5.0 (compat
ible; MSIE 10.0; Windows NT 6.1; Trident\/6.0; {D9D54F49-E51C-445e-92F2-1EE3C2313240}; .NET4.0C; .NET4.0E; 360SE)", "host": "[redacted]",
"code": 200, "time": 1410771195 }
{ "src": "221.232.69.6:3112", "dst": "[redacted]", "method": "GET", "url": "\/cms\/index.php?m=poster&c=index&a=show&siteid=1&spaceid
=18&id=18", "host": "[redacted]", "user-agent": "Mozilla\/5.0 (Windows NT 5.1) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/34.0.1847
.131 Safari\/537.36", "referer": "[redacted]/", "cookie": "UCFDATA=1[redacted]c: ACTION78=1", "code": 20
0, "time": 1410771195 }

三 访问日志(HTTP/HTTPS)&WEB 服务器日志

数据源:出口流量镜像　　工具:E.L.K





四 主机层

数据源:主机IDS-OSSEC

展示界面

文件变更
端口变化
SYSLOG告警

五 网络边界

NMAP / 域名变更通知

对外端口开放情况

对外域名开放情况

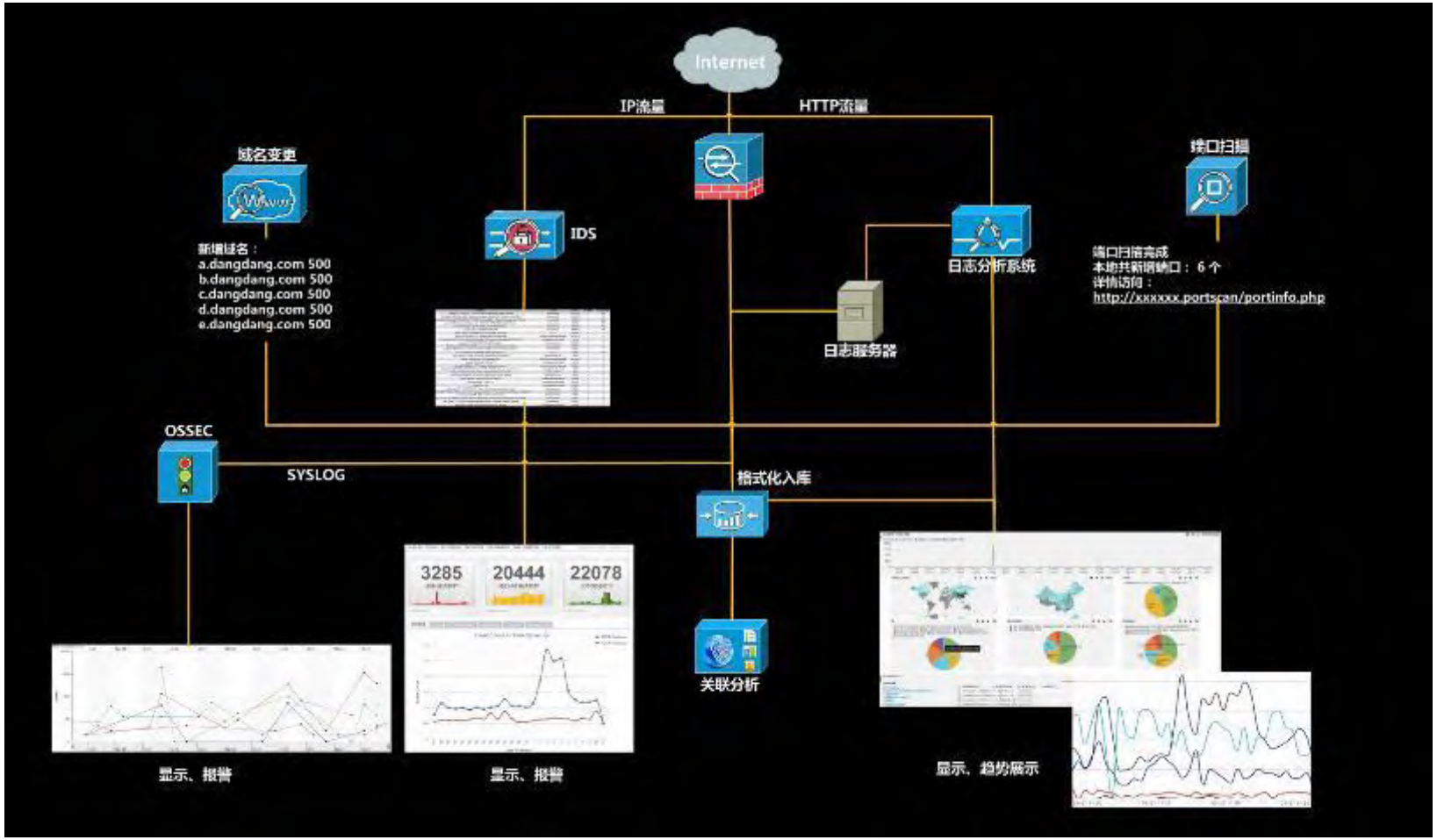

端口扫描 端口状态检测

Show 10 entries Search:

ID	任务ID	插入时间	IP地址	端口	服务	状态	协议	服务标识	服务版本	协议版本
20		2015-04-08 15:47:04	116.213.95.27	80	http	open	tcp	wxws/1.0	None	None
15		2015-04-08 15:46:50	116.213.95.20	443	http	open	tcp	nginx	None	None
18		2015-04-08 15:46:50	116.213.95.25	80	http	open	tcp	Apache httpd	2.2.15	(CentOS)
19		2015-04-08 15:46:50	116.213.95.25	443	http	open	tcp	Apache httpd	2.2.15	(CentOS)
12		2015-04-08 15:46:46	116.213.95.17	80	http	open	tcp	nginx	None	None
13		2015-04-08 15:46:46	116.213.95.17	443	http	open	tcp	nginx	None	None
14		2015-04-08 15:46:46	116.213.95.18	443	http	open	tcp	nginx	None	None
2		2015-04-08 15:46:45	116.213.95.5	80	http	open	tcp	nginx	1.2.4	None
3		2015-04-08 15:46:45	116.213.95.5	443	http	open	tcp	nginx	None	None
5		2015-04-08 15:46:45	116.213.95.10	80	http	open	tcp	nginx	None	None

六 审计设备

数据库审计
BASH 审计
。 。 。


Internet
IP流量
HTTP流量
域名变更
新增域名：
a.dangdang.com 500
b.dangdang.com 500
c.dangdang.com 500
d.dangdang.com 500
e.dangdang.com 500
IDS
日志分析系统
日志服务器
端口扫描
端口扫描完成
本地共新增端口：6个
详情访问：
http://xxxxxx.portscan/portinfo.php
OSSEC
SYSLOG
格式化入库
关联分析
3285
20444
22078
显示、报警
显示、报警
显示、趋势展示

有了以上这些，是否就已经足够了？

工具开发

策略优化

告警调整

性能调整

工具开发

Name	IP	Reason
AutoBladd101	218.247.215.252	SQLMAP FOUND
AutoBladd103	221.0.21.253	Bash Remote Command Execution
AutoBladd104	182.118.33.6	360 WEB SCAN
AutoBladd105	218.30.118.79	360 WEB SCAN
AutoBladd106	182.118.33.7	360 WEB SCAN
AutoBladd107	182.118.33.8	360 WEB SCAN
AutoBladd108	117.26.195.209	Maybe Shell
AutoBladd109	60.180.131.82	Maybe Shell
AutoBladd110	123.125.160.216	360 WEB SCAN
AutoBladd111	74.219.225.231	Bash Remote Command Execution

客户端信息

这些是客户端相关数据

Agent_ID	IP地址	计算机名	文件Hash/最后修改时间(Windows)	连接时间	更新时间	目录大小	操作系统
72	10	hagroxy01	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-07 17:56:05	2015-03-29 18:04:00	3.0M /apps/svac	Linux
73	10.1	hagroxy02	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-11 11:03:44	2015-03-29 18:02:24	3.0M /apps/svac	Linux
5	10.1	XDI-admin_bak	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-11 11:03:24	2015-03-29 18:00:00	3.1M /apps/svac	Linux
10	10	XDI-mongodb	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-11 11:03:28	2015-03-29 18:00:00	3.1M /apps/svac	Linux
18	10	XDI-HA3	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-11 11:03:29	2015-03-29 18:00:00	3.2M /apps/svac	Linux
25	10	E02-Feb02	cc1829e6ee073a01fbdc4fb3ec5892fd	2014-07-11 11:03:32	2015-03-29 18:00:00	5.7M /apps/svac	Linux

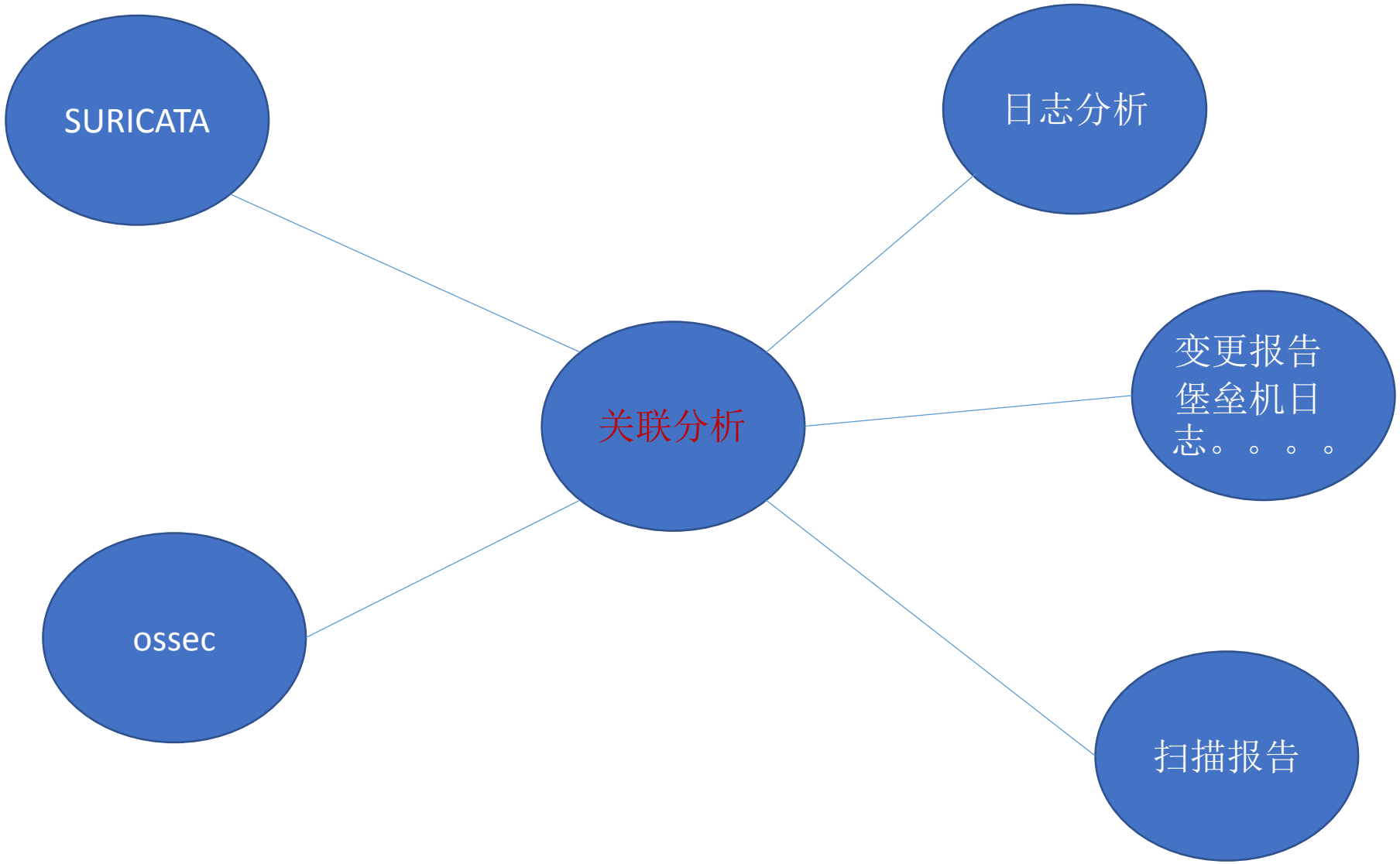
策略优化

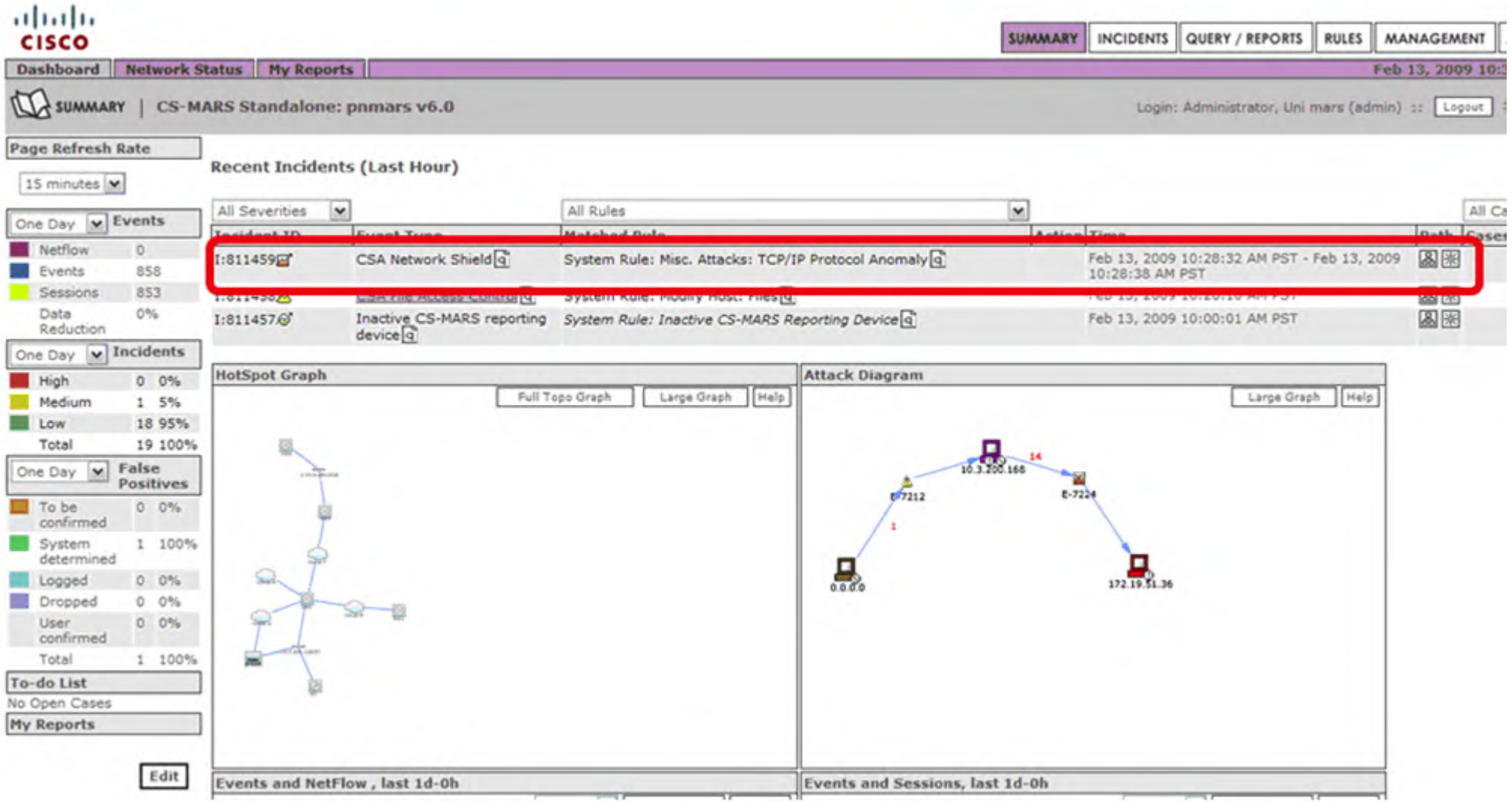
了解常见的黑客软件的签名

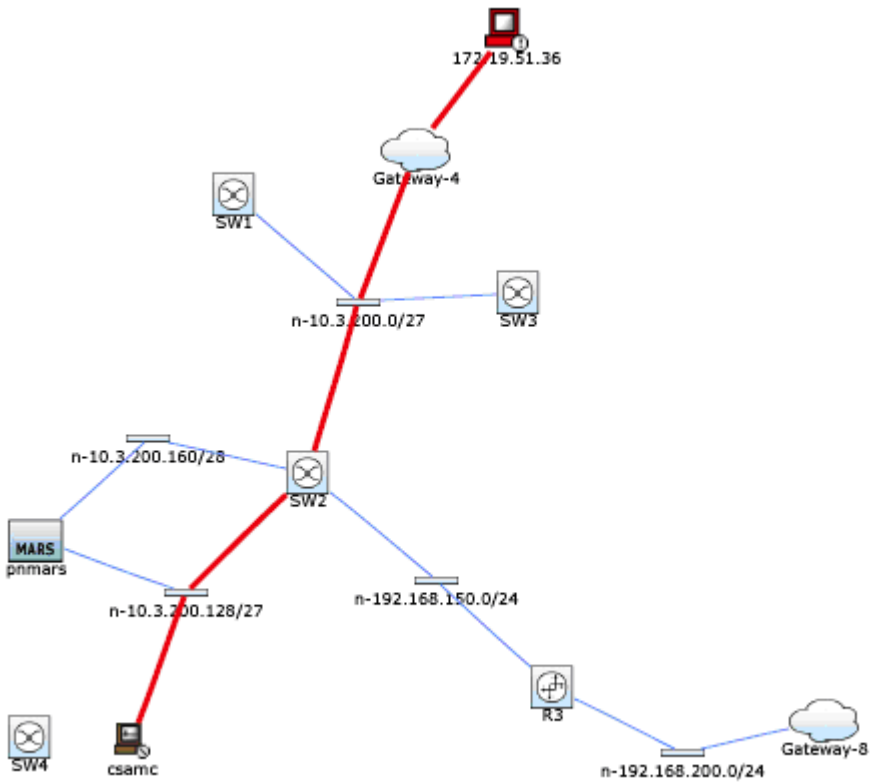
了解安全工具的相关特性

```
alert tcp any any -> any 80 ( sid:900001; content:"base64_decode";
http_client_body;flow:to_server,established; content:"POST"; nocase;
http_method; ;msg:"Webshell Detected Apache";)
```

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg: "China Chopper with all Commands Detected"; flow:to_server,established;
content: "FromBase64String"; content: "z"; pcre: "/Z\d{1,3}/i"; content:"POST"; nocas
reference:url,http://www.fireeye.com/blog/technical/botnet-activities-research/2013/0
breaking-down-the-china-chopper-web-shell-part-i.html;
classtype:web-application-attack; sid: 900000102;)
```


SURICATA
日志分析
关联分析
变更报告
堡垒机日志。。。。
ossec
扫描报告


CISCO
SUMMARY
INCIDENTS
QUERY / REPORTS
RULES
MANAGEMENT
Dashboard
Network Status
My Reports
SUMMARY | CS-MARS Standalone: pnmars v6.0
Login: Administrator, Uni mars (admin) :: Logout
Page Refresh Rate
15 minutes
Recent Incidents (Last Hour)
All Severities
All Rules
One Day Events
Netflow 0
Events 858
Sessions 853
Data Reduction 0%
One Day Incidents
High 0 0%
Medium 1 5%
Low 18 95%
Total 19 100%
One Day False Positives
To be confirmed 0 0%
System determined 1 100%
Logged 0 0%
Dropped 0 0%
User confirmed 0 0%
Total 1 100%
To-do List
No Open Cases
My Reports
Edit
I:811459 CSA Network Shield System Rule: Misc. Attacks: TCP/IP Protocol Anomaly Feb 13, 2009 10:28:32 AM PST - Feb 13, 2009 10:28:38 AM PST
I:811457 Inactive CS-MARS reporting device System Rule: Inactive CS-MARS Reporting Device Feb 13, 2009 10:00:01 AM PST
HotSpot Graph
Full Topo Graph
Large Graph
Help
Attack Diagram
Large Graph
Help
10.3.200.168
E-7212
E-7224
0.0.0.0
172.19.51.36
14
1
Events and NetFlow , last 1d-0h
Events and Sessions, last 1d-0h


172.19.51.36
Gateway-4
SW1
n-10.3.200.0/27
SW3
n-10.3.200.160/28
SW2
MARS
pnmars
n-10.3.200.128/27
n-192.168.150.0/24
R3
SW4
csamc
n-192.168.200.0/24
Gateway-8

告警调整

AV-FREE-FEED Bruteforce attack, SSH authentication attack against DST_IP
Delivery & Attack, Bruteforce Authentication, SSH

▼ RULES

NAME	RELIABILITY	TIMEOUT	OCCURRENCE	FROM	TO	DATA SOURCE	EVENT TYPE	[...]
SSH service authentication attempts failed detected	4	None	1	ANY	ANY	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	6	1800	1	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	6	1800	10	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	6	1800	20	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	8	3600	50	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	8	30000	100	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication attempts failed detected	8	43200	500	1:SRC_IP	1:DST_IP	ossec-authentication_failures (7012)	SIDs: 5712	More
SSH service authentication successful detected	10	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More
SSH service authentication successful detected	10	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More
SSH service authentication successful detected	10	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More
SSH service authentication successful detected	7	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More
SSH service authentication successful detected	2	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More
SSH service authentication successful detected	0	10	1	1:SRC_IP	1:DST_IP	ossec-authentication_success (7009)	SIDs: 5715	More

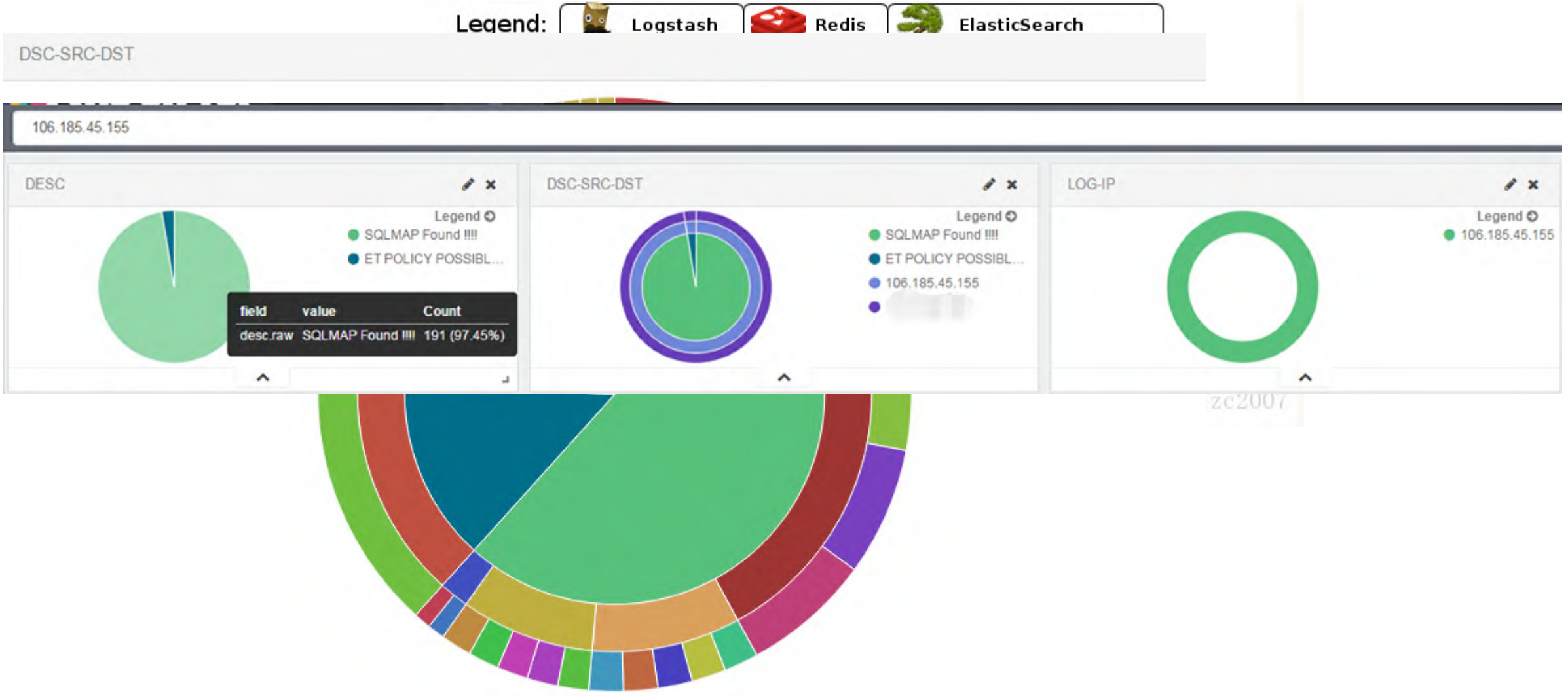
检测内容：

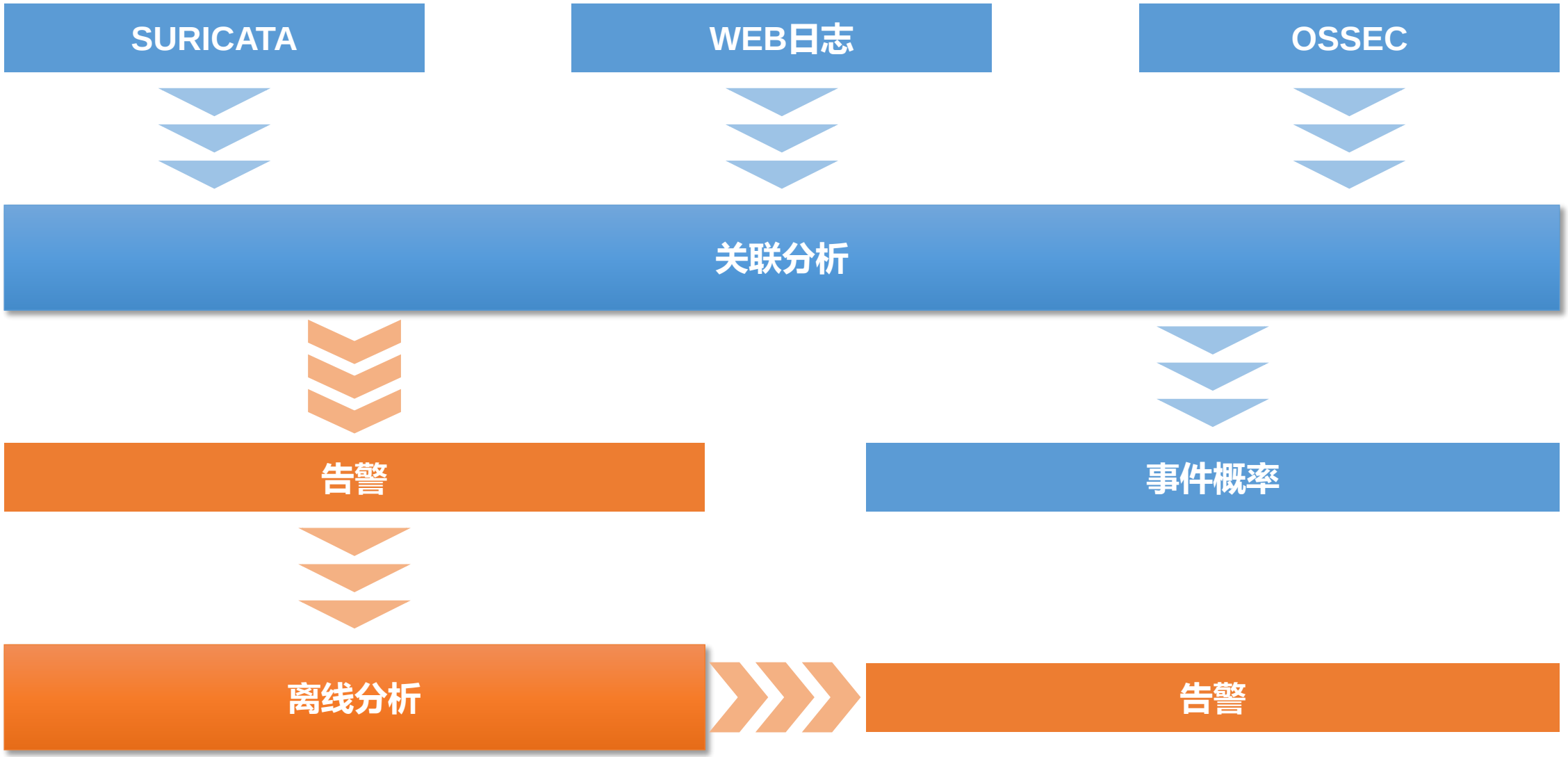
- IP访问频率
- URL访问频率

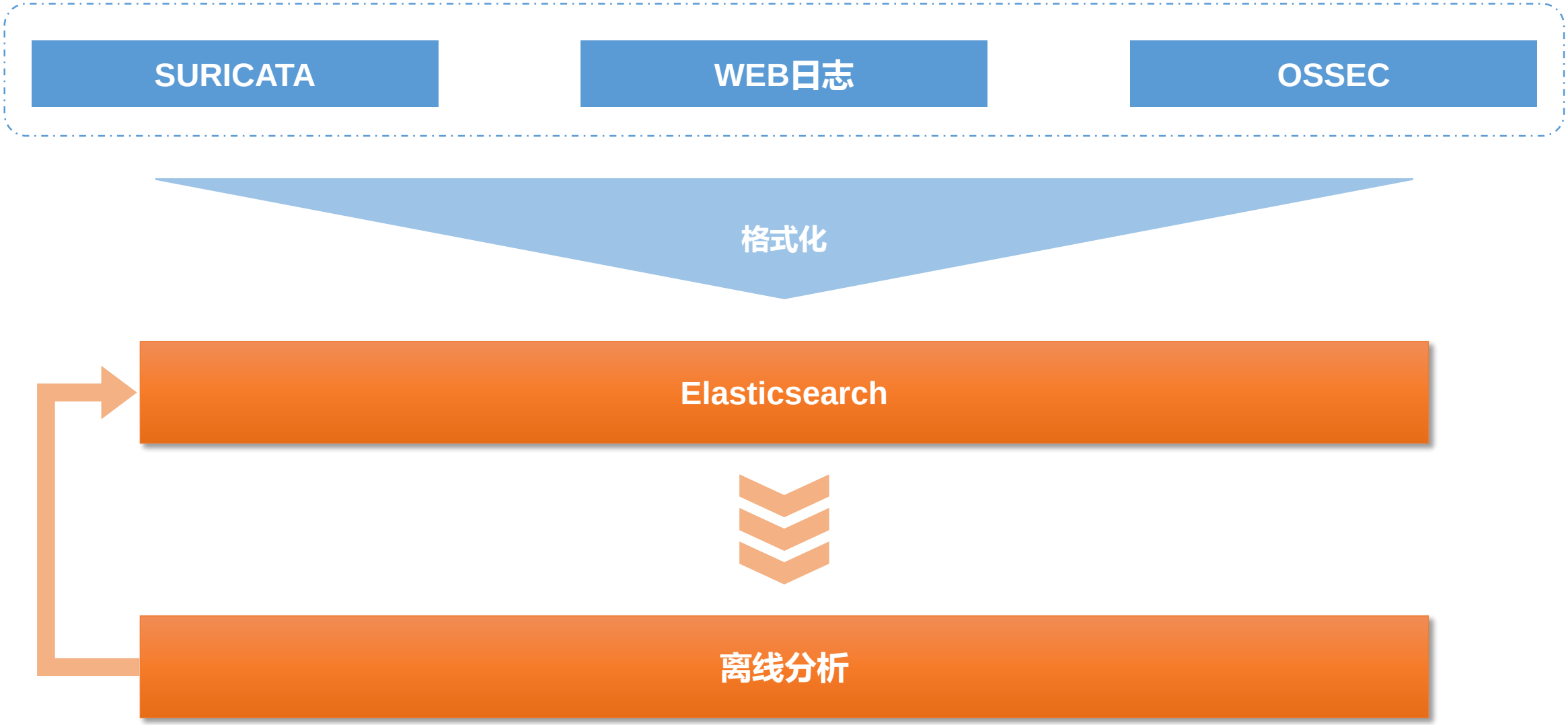
检测恶意行为：

- 扫描/爬虫
- 暴力登录
- 平行权限

关于E.L.K


Legend:
Logstash
Redis
ElasticSearch
DSC-SRC-DST
106.185.45.155
DESC
Legend
SQLMAP Found !!!!
ET POLICY POSSIBL...
field value Count
desc.raw SQLMAP Found !!!! 191 (97.45%)
DSC-SRC-DST
Legend
SQLMAP Found !!!!
ET POLICY POSSIBL...
106.185.45.155
LOG-IP
Legend
106.185.45.155
zc2007


SURICATA
WEB日志
OSSEC
关联分析
告警
事件概率
离线分析
告警


SURICATA
WEB日志
OSSEC
格式化
Elasticsearch
离线分析

采用的关键技术


hadoop


elastic


logstash


APACHE
STORM™
Distributed • Resilient • Real-time

谢谢大家